REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Claims 1, 7, 14 and 18 have been amended.

A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

Claims 1-20 remain pending in this application.

Rejection under 35 U.S.C. § 102

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereafter "Brickell"). Applicant respectfully traverses this rejection for at least the following reasons.

Independent claim 1 is directed to a signature calculation system by use of a mobile agent, where the system comprises a base host and remote hosts in a network. Each of the remote hosts includes a partial signature calculation means. The partial signature calculation means calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent based on data input to the partial signature calculation means, namely (1) signature target data, where the signature target data is target data to which a digital signature of the owner is to be attached, (2) data which have been carried by the mobile agent including partial signature auxiliary data, where the partial signature auxiliary data is generated in the base host based in part on a secret key of the mobile agent owner, and (3) a secret key of the remote host. Brickell fails to disclose a partial signature calculation means that calculates a partial signature in a remote host based on input data, where the input data falls into either category (1) or (2) above.

Brickell discloses a multi-step digital signature system having a distributed root certifying authority (abstract). The system includes a distributed root certifying authority 20 which includes a set of RCA members 22-30 (Fig. 1, col. 5, lines 36-39). In the signature process of Brickell, an RCA administrator receives a message (which may be a certificate) for signature, and the message is distributed to each of n RCA members (col. 11, lines 18-21). When signing the message, each RCA member separately applies a key fragment to the message without recombining the shares to form a whole key (col. 7, lines 20-22). Each of the RCA members in a key generating group, RCA_{Bi}, selects a random number (x_{Bi}) between 1 and q-1 which is taken to be the private root key fragment for that member (col. 20, lines 22-26). Each of the RCA members computes separate values r_i, s_i, based in part, on the RCA members selected random number k_i (col. 11, lines 31-38, col. 12, lines 26-32). Each RCA member also may calculate a value t based on a composite r of the r_i values (col. 12, lines 16-25). The s_i values are distributed to a common entity, which computes a composite S of the s_i and the entity attaches the signature (t,s) to the message.

While Brickell discloses computing a signature (t,s) which is based on a number of individual values r_i and s_i calculated by the individual RCA members based on individual keys of the RCA members, Brickell does not disclose a system including a base host and remote hosts, where the partial signatures are computed based on data input into the RCA members where that data falls into either category 1) signature target data, where the signature target data is target data to which a digital signature of the owner is to be attached, or 2) data which have been carried by a mobile agent including partial signature auxiliary data, where the partial signature auxiliary data is generated in the base host based in part on a secret key of the mobile agent owner. The individual values r_i and s_i are not calculated based on data falling into categories 1) or 2). Thus, Brickell does not anticipate claim 1.

With respect to the limitation of the remote host in the claims, which includes the partial signature calculation means, the Office Action cites to Brickell at col. 7, line 36 to col. 9, line 9. For the reasons given above, applicants submit that Brickell does not disclose all the features of the partial signature calculation means either in the cited section of Brickell or anywhere else. If the present rejection based on Brickell is maintained, the Examiner is respectfully requested to specifically point out by specific column and line number where Brickell specifically discloses the limitations of the partial signature calculation means in the next Office Action.

Moreover, while in the Brickell system fragments of keys are always used in generating a signature in a device (Signing Unit 70), the present invention as claimed allows for input of an encrypted text of the fragments (partial signature auxiliary data) into a remote host when a signature is generated. Consequently, in the invention as claimed, the remote host need not possess a private key for generating a signature, and it becomes easier to control keys. This feature is not suggested by Brickell.

Independent claims 7, 14 and 18 are likewise patentable over Brickell. Claims 7, 14 and 18 respectively recite "a partial signature calculation means to which signature target data, the signature target data being target data to which a digital signature of the owner is to be attached, data which have been carried by the mobile agent including the partial signature auxiliary data, and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent", "a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, the signature target data being target data to which a digital signature of the owner of the mobile agent is to be attached, data which have been carried by the mobile agent including partial signature auxiliary data which has been generated based on generated random numbers and a secret key of the owner at a base host, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data", and "a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, the signature target data being target data to which a digital signature of the owner of the mobile agent is to be attached, data which have been carried by the mobile agent including partial signature auxiliary data which has been generated based on generated random numbers and a secret key of the owner at a base host, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data." Thus, claims 7, 14 and 18 are patentable for reasons analogous to those above with respect to claim 1.

Claims 13 and 17 respectively recite "generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts" and "generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of a mobile agent." These features are not disclosed in Brickell, and thus claims 13 and 17 are patentable thereover.

The dependent claims depend from one of the respective independent claims, and are patentable for at least the same reasons, as well as for further patentable features recited therein.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date July 18, 2005

By Thomas G. Bilodeau

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Thomas G. Bilodeau
Attorney for Applicant
Registration No. 43,438